Intro Remarks

Good afternoon Madame Chair and Members. My name is Sarah Boot and I'm testifying on behalf of CalChamber. We represent California businesses across every industry, including over 14,000 small businesses.

As you all know, the CCPA passed through the legislative process in just one week due to the impending deadline to remove the initiative from the ballot. There was not an opportunity for diverse stakeholder input, and the result is a law that can be confusing and that presents some serious privacy concerns and operational challenges.

Last June, when this law was passed, the fact that it needs fixes was not controversial. The authors noted there would need to be some fixes. And numerous legislators signed a letter stating that while they agreed with the bill's expansion of privacy rights -they were concerned with how quickly it passed – and expected to work on reasonable fixes going forward.

Unfortunately, since that time, there's been a narrative that any changes to this law requested by business would be rolling back privacy rights. But that's not true.

Size of Biz Impacted

And the narrative that this law only applies to big tech and data brokers isn't true either. The CCPA applies to a third, very broad category of businesses: any business that annually *receives* the personal information of 50,000 or more consumers, households, or devices.

It turns out, 50,000 pieces of data is not a lot given that one consumer can be counted multiple times and given the CCPA's broad definition of personal information, which includes IP addresses and so much more.

For example, the CCPA applies to businesses with 50,000 website visitors per year. If a business has an average of 137 unique online visitors per day, it will hit the threshold. And just think of all the small businesses that easily conduct an average of 137 transactions per day – which is about 12 transactions per hour in a 12-hour day - convenience stores, coffee shops, restaurants... there are so many.

The point is that the CCPA covers a great many businesses and treats them all the same as the handful of tech giants in this state.

Please keep the diversity of these businesses in mind as I outline our concerns today – and please keep an open mind. I am going to start by discussing 5 fixes necessary to protect consumer data security, privacy, and choice.

Specific Pieces of Info

First, the CCPA requires businesses to provide consumers "specific pieces of information" the business has collected after receiving a consumer request. But, specific pieces of information is not defined. It could mean that businesses must transmit highly sensitive information back to consumers, like credit card numbers or specific internet searches. Information that consumers already know about themselves.

This would create a risk of fraudsters posing as the consumer to get access to this data. To alleviate that risk, a business may need to collect even more information from the requesting consumer to be sure it is sending sensitive information to the right person – especially when a business has no direct relationship with the consumer. This runs counter to privacy goals and could greatly harm consumers. So, we are requesting a CCPA amendment to limit these risks.

Households/Devices

Second, the CCPA's references to households and devices in the definition of personal information also presents serious risks. As drafted, one member of a household – whether they are an abusive spouse or a roommate – seems to be able to access all of the specific pieces of information – including credit card info or precise geolocation data – about another member of their household. For example, a household member may request access to specific pieces of information from a grocery store delivery service, thereby exposing another household member's purchase of sensitive items, like a pregnancy test.

Similarly, one user of a device can request all of the specific pieces of information a company has about that particular device, which could reveal private things about another user of the device.

The inclusion of households and devices could also infringe on the choices of others. For example, if one household member makes a request to delete all data associated with a household, another household member would be subsequently unable to access their information.

Personal Info/Deidentified/Publicly Available

Third, the definition of personal information is incredibly overbroad – if not adjusted, it will undermine existing privacy-protective practices and impose significant operational costs on businesses.

Most people think of personal information as data that could identify someone, like birthdates or social security numbers. The CCPA defines "personal information" far more broadly, as "information that . . .identifies, relates to, describes, is capable of being associated with, or could reasonably be linked to . . . a particular consumer or household."

Oddly, this definition creates a reasonableness standard for data that can be linked to a person or household – but it does not make the same allowance of reasonableness for data that is "capable of being associated with" them. As a practical matter, this means "personal information" under the CCPA is any information that COULD IN THEORY BE associated with a person or household.

Let's put this into context. If I have an online account with a store and I exercise my rights under CCPA, that store should be able to provide me with my account details or to delete them.

But that's only the beginning of what a business is required to do under this law. Let's say I also browse sales on the store's website or fill up shopping carts without logging in – and that store keeps IP addresses to track how consumers use their website, but it doesn't link that data back with a person. Under the CCPA, the store could be required to search for every possible IP address they have that could in theory be linked back to me. Similarly, if I made purchases inside their brick and mortar store, they could be required to search security camera footage to find where I appear on it.

The only way for businesses to comply would be to identify people interacting with their business and to store that information together in one place, which would be hugely wasteful and harmful to consumer privacy.

We don't believe this was the result intended. The law has an exemption stating that a business is not required to relink data that is "not maintained in a manner that would be considered personal information." But under the definition of personal information basically all data is personal information. So this exemption does not provide relief, and should be fixed.

Finally, although the definition of personal information is pretty all-encompassing, there are three types of data that we believe are NOT meant to be personal information under the law: deidentifed data, aggregate data, and publicly available data. But even these exemptions need adjustments to be meaningful.

Under the current definition of deidentified only aggregate data could ever qualify as deidentified, which would discourage businesses from using this privacy protective practice.

Additionally, the definition of publicly available information is limited to government records – and then further restricted to such records that are used for a purpose that is compatible with the purpose for which the government data is maintained publicly. Aside from being confusing

and thus inviting unnecessary litigation - this restriction is an unconstitutional limit on free speech and must be removed from the law.

Loyalty/Rewards Programs

Fourth, confusing language in the non-discrimination section – raises doubts about the legality of loyalty and rewards programs offered by retailers, grocers, hotels and airlines. Consumers love these programs – in fact, 80% of Americans belong to at least one. While we understand the legislative intent is that businesses can continue to offer them, unless this section is clarified, it will be up to the courts to determine the fate of these programs – and there's no need for that level of uncertainty.

Fraud/Gov't Programs

Fifth, the CCPA also needs to be clarified to prevent bad actors from opting out of data services used to implement crucial government programs as well as to prevent identity theft and money laundering.

I'm now going to discuss two areas of this law that will lead to unnecessary compliance costs for businesses and unintended consequences if not fixed.

Consumer Definition

First, the definition of consumer is any California resident, and without clarification, this could be interpreted to include employees. The operational costs for businesses – especially small businesses – of including employees and job applicants will be exorbitant. Imagine a family-owned restaurant that serves 150 tables a day –without fixing this definition it may have to operationalize the CCPA for its kitchen and wait staff in a business with high turnover and low profit margins.

Access to personal information in the employment context is already established in California law. But the CCPA would allow a separated spouse who is part of a household to gain access to payroll records. That cannot be what the legislature intended.

The definition of consumer is also problematic because it includes business representatives in the context of business to business interactions. For example, a small medical practice that already complies with HIPAA for patient data, would be required to honor opt out and deletion requests from suppliers with whom they email for business purposes but who never have access to patient data. If not fixed, this will lead to unfortunate unintended consequences.

Online Ads

Second, targeted, online advertising is another area that CCPA was not intended to impact. However, the current language lacks clarity. Online advertising is a privacy protective practice in which no personally identifiable information is being sold. The internet ecosystem depends on this--from small blogs to large publications, including our favorite newspapers. And businesses of all sizes depend on this advertising network to reach consumers. This important area deserves clarification.

Closing

Finally, I will address enforcement. The CCPA creates an onerous private right of action to sue businesses that have suffered a data breach – no proof of injury is required and the minimum statutory damages awarded could put folks out of business.

There should be a safe harbor for businesses that have implemented recognized security standards – but there isn't.

Despite this, and despite the other flaws with this law, the business community encouraged legislators to vote for it – which resulted in the unanimous vote. We did this because we hoped we could fix some of the problems I've mentioned and because the PRA was limited to the data breach provisions of the law.

This law is complicated, it can be confusing, it's not finished, and it applies to businesses of all sizes. I've been on calls with privacy experts from around the country who disagree about what certain provisions mean. We should not further expand the PRA to have trial attorneys enforce more of this law – which was largely pulled from a regulatory model. The abuses we've seen with PAGA would pale in comparison.

In closing, let's not lose sight of the fact that we've just passed the most robust privacy law in the country. Compliance with this law will be incredibly expensive. We don't yet know the impact this will have on our economy or how it will raise prices on consumers. These are crucial factors legislators need to consider before adding even more onerous burdens on top of the CCPA.

Thank you.